

Cloud Computing: Introduction to Cryptography

Er. Rasneet Kaur Chauhan, Er. Sharanjit Singh

Department of CSE,

Guru Nanak Dev University RC Gurdaspur,

Punjab, INDIA.

Abstract: Users connect the cloud they seen cloud as a single application, device, or document. All things inside the cloud system like hardware in the cloud and the operating system that manages the hardware connections are invisible. Cloud Computing is evolving very fast. It is considered as the next generation architecture for computing. Thus cloud computing is a combination of several computing resources that can be accessed via internet. Several IT professionals agree that cloud computing is the most revolutionary information delivery model since the introduction of the Internet. For the decision makers and corporate management, cloud computing has bring huge functional and financial benefits as well as many serious security concerns that threaten the business continuity and the corporate reputation. The definition of cloud computing is still not clear and blurry in large part, due to the magnitude of the security risks and virtually unlimited amount of the data and information that is being published. Hence, the organizations and clients used to store data in the data centers with a firewall and other security techniques that are used to protect their data against intruders to access the data.

Keywords: Cloud Computing; Security; Service Models; Components.

I. INTRODUCTION

Cloud Computing is the name given to the recent trend in computing service provision. This trend has seen the technological and cultural shift of computing service provision from being provided locally to being provided remotely by some third-party service providers. Cloud Computing has become one of the most talked about technologies in recent times and has got lots of attention from media as well as analysts because of the opportunities it is offering. On the surface, cloud computing seems to increase IT agility by eliminating many of the wearying tasks and responsibilities that IT departments manage these days. IT departments have been integrated so deeply into core businesses that most business operations would halt without the services and infrastructures that IT teams maintain. Furthermore, the fundamental challenges and responsibilities of IT will never stop growing, as the business and the regulatory requirements become much more complex, a stronger protection from security threats become virtually mandatory, and technologies themselves become more ubiquitous, hence skill- and time-intensive. Therefore, traditional IT teams are frequently forced to devote a large portion of their time and budgets to tasks that are not directly tied to revenues, and added values that must be clearly visible to top management. To build trust for growth of the cloud computing, cloud providers must protect user data from all unauthorized accesses and other disclosures. Several techniques can be used for this purpose. One technique is to encrypt the data on the client side before storing it in the cloud storage, this technique has tremendous burden from the client perspective in terms of key management and maintenance perspective etc. The application or software will provide data integrity verification by using hashing algorithm, provide encryption/decryption by some symmetric and asymmetric algorithms, and group of people that access the shared data securely can be achieved by making some access list.

II. CRYPTOGRAPHY: OVERVIEW

Cryptography, also called as the study of secret, however these days it is mostly attached to the definition of the encryption. Encryption is a process by which we convert the plain text which is "unhidden" to some cryptic text "hidden" so as make it secure against the data attackers and thieves. This process has other side also where the cryptic text is decrypted on the other end for its understanding. Following figure shows a simple flow of the commonly used encryption algorithms.

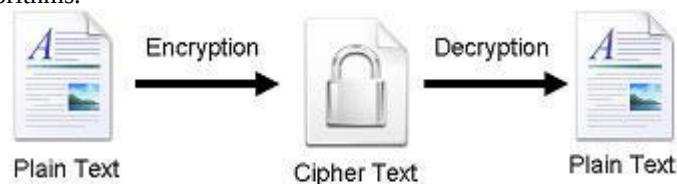


Fig.1 Encryption-Decryption Flow

A. Block Ciphers and Stream Ciphers

One of the important categorization methods that is used for the encryption techniques commonly used is based on the form of the input data that they operate on. These are called Block Cipher and Stream Cipher. Here, we will discuss the main features in these two types, their operation mode, and at last compare them in terms of the security and performance.

• Block Cipher

Before describing the key characteristics of a block cipher, the definition of cipher word must be given. A cipher is an algorithm which is used for performing the encryption and the reverse is decryption.

In this method, the data is encrypted and then decrypted if the data is in the form of blocks. In its simplest way, you may divide the plain text into blocks and then they are fed to the cipher system to produce different blocks of the cipher text.

ECB i.e. Electronic Codebook Mode is a simplest form of block cipher where data blocks are encrypted directly so as to generate its corresponding ciphered blocks.

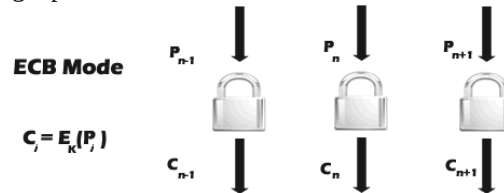


Fig.2 Block Cipher ECB Mode.

• Stream Ciphers

Stream cipher functions on a stream of data by operating it bit by bit. Stream cipher majorly consists of two major components i.e. a key stream generator and a mixing function. Mixing function is just an XOR function and the key stream generator is the main unit in the stream cipher encryption technique. Example, if the key stream generator generates a long series of zeros, the output ciphered stream would be similar to the original text. Figure below shows the operation of the simple mode in a stream cipher.

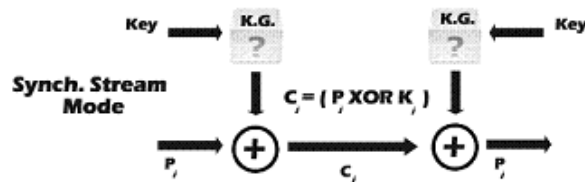


Fig. 3 Stream Cipher (Simple Mode)

III. ENCRYPTION TECHNIQUES

Data encryption procedures are mostly divided into two categories that depend on the type of security keys which are used to encrypt or decrypt the secured data. These categories are: Asymmetric and Symmetric encryption techniques

• Symmetric Encryption

In this type of encryption, the sender and receiver both agree for a secret shared key shared by both. They use this secret key for encrypting and decrypting of their sent messages. Figure shows the process of symmetric cryptography. Both the nodes firstly agree on a specific encryption technique that will be used in encryption and the decryption of data sent. They both agree on the secret key that they both will be using in this connection. After this encryption finishes, node A then starts sending its data that is encrypted with the shared key, and the node B uses that same key to decrypt that encrypted messages.

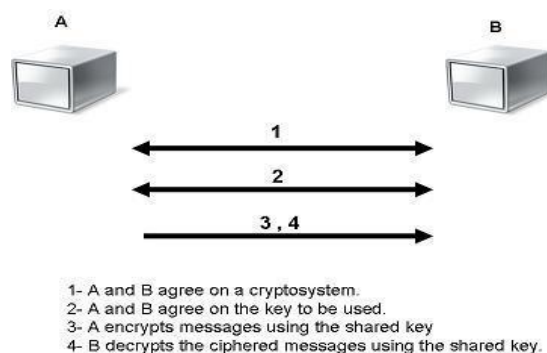


Fig.4 Symmetric Encryption

- **Asymmetric Encryption**

Asymmetric encryption is another type of encryption where two keys are used. To explain this, what Key1 has encrypted can only be decrypted by Key2, and vice versa. It is also called as the Public Key Cryptography, PKC, because the users use two keys i.e. public key that is known to the public, and the private key that is known to the user only.

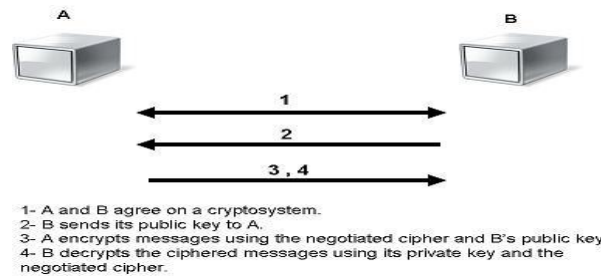


Fig.5 Asymmetric Encryption

- **Hash Function Cryptography**

The hash function cryptography or One way cryptography offers a different way of creating some fixed-size blocks of data by making use of the entry data with some variable length. It is also known as taking of digital fingerprint of the data, and exit data are called as the message digest or a one-way encryption. If the data is modified after a hash function was generated, hence the second value of the hash function of data is not the same.

IV. CRYPTOGRAPHIC ALGORITHMS

- **Data Encryption Standard (DES)**

The Data Encryption Standard (DES) is a symmetric key block cipher which was published as FIPS-46 in a Federal Register in January 1977 by National Institute of Standards and Technology. At the encryption side, it takes a 64-bit plaintext and hence creates a 64-bit ciphertext, at other side i.e. decryption side it takes the 64-bit ciphertext and in return creates a 64-bit plaintext, and the same 56 bit cipher key is used for both encryption process and decryption process.

- **Advanced Encryption Standard (AES)**

Advanced Encryption Standard is a symmetric key block cipher technique that was published as FIPS-197 in Federal Register in December 2001 by National Institute of Standards and Technology (NIST). This is a non-Feistel cipher. It encrypts the data with a block size of 128-bits.

- **Triple-DES**

An easy way of increasing the key size of DES is by using Triple DES so as to guard it against the attacks without designing a completely new block cipher algorithm. It is thus an enhancement version of DES. It also removes the man-in-the-middle attack occurred in 2-DES.

- **RSA**

RSA is a public key algorithm that is based on the difficulty of prime factorization. Similar to most of the public key password features, RSA password is also block encrypted, but is different from other block encryption which are used in a secret key algorithm like DES (Data Encryption Standard) in the way that the length of the plain text and a key is a variable; hence in other words, a relatively long length of the key can also be used for considering of a reliable and secure system, which is a relatively short length of key that is used for an efficient system.

- **Blowfish**

It uses a block cipher of 64-bit block and a key of variable length that ranges from 32 bits to 448 bits. It is one of the public domain encryption algorithms. Blowfish algorithm was designed by Bruce Schneider in 1993 as a fast alternative to the existing encryption algorithms. Blowfish has around 16 rounds or less. Blowfish is a highly secure cipher and uses encryption that is free of patents and copyrights. No attack is yet successful against Blowfish, though it suffers from the weak keys problem.

V. COMPARISON OF ALGORITHMS

In this section, we are giving comparison of all the cryptographic algorithms used. We will start with the main types of classification. Comparison of symmetric, asymmetric and hash function has been given in general. The symmetric, asymmetric key cryptography techniques are much complex and thus take more time. Hence, if delays are more than the security risks are also more. On the other hand, hash function cryptography is not complex. It takes much less time for execution than above two. Thus if it takes less time means then delays are also less and the security risks are less too.

- **General encryption and decryption time**

The files of 49, 59, 100, 247, 321, 694, 899, 963, 5345.28, 7310.336 all in kb are inputted to all the algorithms

AES, 3DES, DES, RSA, BlowFish and then their general execution time for encryption and decryption is noted. The results of this analysis are as follows:

Input size in (Kbytes)	AES	3DES	DES	RSA	Blow Fish	RC2
47	54	53	31	59	37	57
57	33	46	35	52	39	60
102	96	84	45	94	40	91
245	103	109	48	120	46	121
320	173	163	83	172	47	168
696	216	228	149	232	47	262
896	260	295	242	309	62	268
967	201	289	245	296	63	295
5347.28	1233	1168	1299	1441	120	1570
7312.336	1372	1784	1698	2357	103	1915
Average Time	375	450	385	513.2	60.1	480.7
Throughput (Megabyte s/sec)	4.174	3.45	4.01	1.89	25.892	3.247

Table 1. Execution times (in milliseconds) of encryption algorithms with different packet size

Input size In (Kbytes)	AES	3DES	RSA	Blow fish	DES	RC2
47	64	55	65	35	52	65
57	59	50	63	27	40	59
102	64	59	51	50	56	90
245	72	76	73	68	74	95
320	145	88	148	95	78	161
695	147	142	153	85	124	165
896	174	177	186	100	150	183
967	160	180	193	82	153	194
5347.28	651	837	827	146	786	904
7312.336	886	1104	1176	144	950	1216
Average Time	240	275.9	293.5	83.7	245	313.2
Throughput (Megabytes/sec)	6.452	5.665	3.43	18.72	6.347	4.985

Table 2. Execution times (in milliseconds) of decryption algorithms with different packet size

- **Data files of different sizes with same type.**

In we take different files of same types but different sizes are given for encryption and their encryption time is calculated. Table 2 gives the details about the files used for all executions and Figure 3 and 4 show the execution results for BMP and FLV file formats of different sizes respectively.

File Type	Data Size
BMP	10MB, 55MB, 105MB
FLV	52MB, 105MB, 485MB

Table 3. Files used

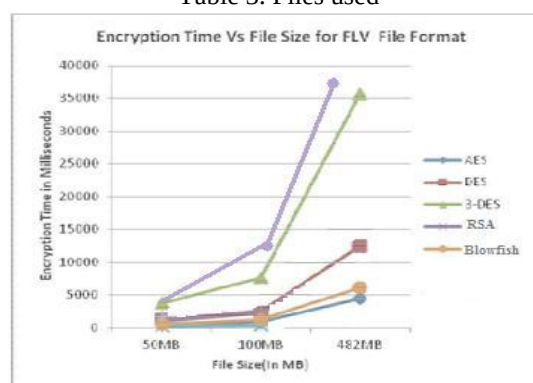


Fig 6. File size Vs Encryption time for BMP file of different sizes

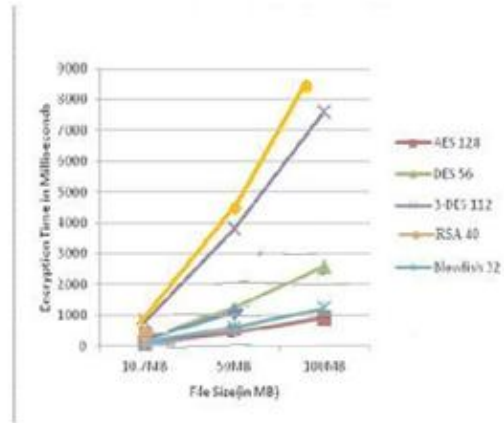


Fig 7. File size Vs Encryption time for FLV file of different sizes.

For each encryption algorithm same parameters are used for files of varying sizes. Hence, the result for different size of data varies proportional to the data file size. Encryption time increases as file size increases in multiples of data size.

VI. CONCLUSION

The purpose of this paper is to assess how security risk factors are affecting the existing cloud users' cloud usage strategies. Organizations that host the critical applications and data in clouds are no longer considered to be early adopters. Are they simply betting that financial benefits will surpass security risks? or are they confident that cloud providers are capable of assuring an equal or higher level of security than on-premise systems?

Examining real-world users' opinions on risks and threats is beneficial to organizations considering adding cloud to their IT portfolio. Security is the top obstacle, other factors such as cost control, availability, and vendor lock-in require extensive research and analysis which is likely to produce less than definitive indicators for decision making. Hence this trend of favoring cost-saving solutions is likely to continue at a rate much more consistent with the growth of cloud adoption. Different kind of cloud computing security issues are discussed here that exploit the security system. Hence, the notion of data privacy is addressed which is impossible to maintain without the security and the degree of trust afforded to a cloud service provider is being analysed. Thus it is required for a cloud service provider to secure a data transmission at specific cloud data centers.

REFERENCES

- [1] Z.Lan, V.Varadharajan and M.Hitchens, "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage", Information Forensics and Security, IEEE Transactions on, vol.8, no.12, (2013), pp. 1947-1960.
- [2] J.Taeho, L.Xiang-Yang, W.Zhiguo and W.Meng, "Privacy preserving cloud data access with multi-authorities", Paper presented at the INFOCOM, 2013 Proceedings IEEE, (2013, 14-19 April 2013).
- [3] Y.Ching-Nung and L. Jia-Bin, "Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing", Paper presented at the Biometrics and Security Technologies (ISBAST), 2013 International Symposium on. (2013, 2-5 July 2013).
- [4] P.Rewagad and Y.Pawar, "Use of Digital Signature with Diffie-Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing", Paper presented at the Communication Systems and Network Technologies (CSNT), 2013 International Conference on. (2013, 6-8 April 2013).
- [5] M.S.Abolghasemi, M.M. Sefidab and R.E.Atani, "Using location based encryption to improve the security of data access in cloud computing", Paper presented at the Advances in Computing, Communications and Informatics (ICACCI), 2013 International Conference on. (2013, 22-25 Aug. 2013).
- [6] Kalpana and Singaraju, "Data Security in Cloud Computing using RSA Algorithm", in International Journal of Research in Computer and Communication technology (IJRCCT), vol.1, no. 4, (2012).
- [7] Q.Liu, G.Wang and J.Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment", Information Sciences, vol.258, (2014), pp. 355-370.